Missouri Division of Credit Unions

NEWSLETTER

Volume 8, Issue 3 **September 25, 2006**

DEPARTMENT OF INSURANCE, FINANCIAL INSTITUTIONS AND PROFESSIONAL REGISTRATION

301 West High Street
Suite 720-A
P.O. Box 1607
Jefferson City, MO 65102

Phone: 573-751-3419
Fax: 573-751-6834
E-mail: cu@cu.mo.gov

Inside this issue:

Division Transfers Departments

Effective August 28th, the Division of Credit Unions has transferred from the Department of Economic Development to the Department of Insurance, Financial Institutions and Professional Registration (DIFP). This transfer occurred as a result of Executive Order 06-04, signed by Governor Blunt on February 1.

According to an August 28th press release from DIFP Director Dale Finke, "We will continue to cooperate together to ensure that there is no interruption of programs or services from any facet of this new department. We are already realizing some of the benefits of sharing our expertise."

Under DIFP, the Division of Credit Unions will continue to operate in an autonomous manner, and the effects of the transfer will be mostly transparent to the credit unions DIFP's website may be viewed at www.difp.mo.gov.

Items that have changed include the Division's website and e-mail addresses. The Division's website has been shortened to www.cu.mo.gov.

E-mail addresses that previously ended in: ded.mo.gov will now be cu.mo.gov.

For example, sandy.branson@cu.mo.gov. The Division's mailing address, physical location and phone numbers are unchanged.

Call Reports

Each credit union will soon or already has received a call report packet from the NCUA. In the past these reports were distributed by the Division. This change was implemented as a cost-cutting practice for the Division, funded by Missouri state chartered credit unions.

Each credit union will also receive a packet from the Division. In this packet will be a letter informing them of the call report change and a form requesting certain contact information. New to this form is a request for a cell phone number as an emergency contact, if possible. This request is part of our disaster recovery plan. Credit union managers can rest assured that this number will only be used in the event of an emergency.

Call reports will be due by October 24th whether it is mailed or sent by e-send.

Data Collection Project

Subsequent to a November 2005 hearing on the tax exemption of credit unions, the United States House Ways and Means Committee chaired by Representative Bill Thomas (R-CA), requested information on credit unions' service to its members. In order to understand how credit unions use their tax-exempt status, this congressional committee has requested information on four areas:

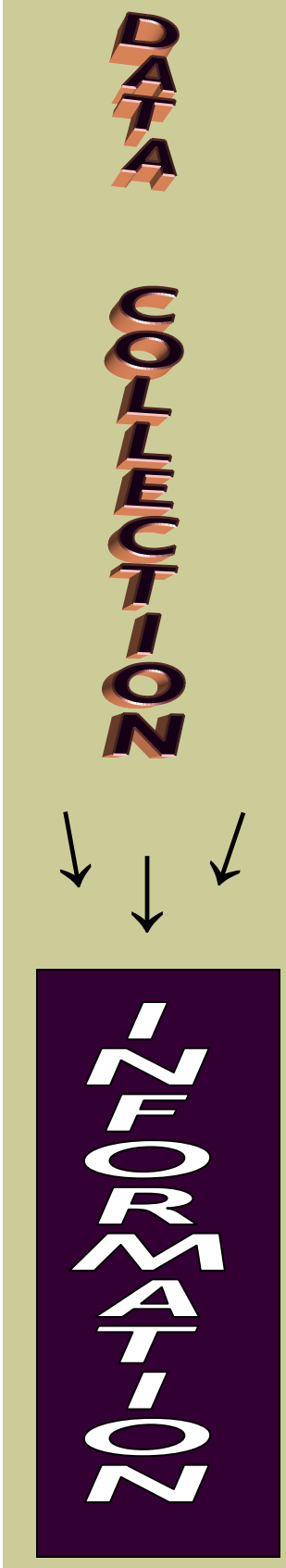
1) the income characteristics of its members;
2) executive compensation;
3) Credit Union Service Organizations and
4) unrelated business income tax.

Data has been collected from federal credit unions by the NCUA. The National Association of State Credit Union Supervisors (NASCUS) is coordinating the project for state-chartered credit unions. While state and federal charters operate under different laws and regulations they both carry an exemption from federal income taxes. One difference exists in the federal and state charters in the sense that the Federal Credit Union Act enacted by Congress details federal credit union's "… mission of meeting the credit and savings needs of consumers, especially people of modest means". The state credit union statutes do not include this term.

Although, many state statutes do not cite the mission of credit unions to serve those of modest means, the House Ways and Means Committee has requested similar information from state chartered credit unions all over the country. All state regulators have agreed to participate in the data collection project.

Only a representative sample of Missouri credit unions will be included in the project. The National Association of State Credit Union Supervisors (NASCUS) has hired a statistician to develop a methodology to determine an accurate sample of state credit unions. Shortly after receiving the selected credit unions, someone from the Division will call each credit union to proceed with the collection of data for this project. An AIRES download will be requested and a questionnaire will be completed with a telephone call.

Confidentiality has been a major consideration in this project. No individual credit union or member information will be divulged. The entire process should not be a material burden to any individual credit union.



AUTHENTICATION

In November 2005, the Federal Financial Institutions Examination Council (FFIEC) and NCUA released changes to privacy and security regulations related to electronic banking (i.e. online banking, telephone banking, etc.) and required mandatory compliance by year end 2006. This guidance was issued under NCUA Letter to Credit Unions 05-CU-18 and most recently 06-CU-13.

Although this guidance addresses risk-based assessments, monitoring / reporting, and member awareness, the primary issue is related to authentication techniques. Essentially, the FFIEC considers "single-factor authentication, as the only control mechanism, to be **inadequate** for high-risk transactions involving access to customer information or the movement of funds to other parties". This "single-factor authentication" refers to, for example, only utilizing a user-id and password when logging onto members' online accounts. Due to the recent growth and popularity of transactional websites and more sophisticated methods for account fraud and identity theft, an effective and reliable authentication system must be implemented to safeguard your members' assets.

In response to this guidance, the Division will be contacting all state-chartered credit unions utilizing electronic banking to ensure all institutions have addressed enhanced authentication techniques by this year-end.

The above referenced guidance requires a completed risk-assessment, enhanced authentication techniques, audit features for monitoring unauthorized activities, and member awareness activities. The following includes a brief summary of each. Please note, this summary is not all-inclusive and since each institution is unique, some credit unions may necessitate additional requirements.

Risk Assessment

Since each credit union's size, complexity, and strategy are all unique, the standards required for each institutions electronic banking authentication program will similarly be unique. Therefore, enhancement of your authentication methodologies must start with an electronic banking risk assessment to determine the level of authentication appropriate for your credit union's particular applications.

This risk assessment should:

- Identify all transactions and levels of access associated with electronic banking customer products and services;
- Identify and assess the risk mitigation techniques, including authentication methodologies, employed for each transaction type and level of access; and
- Include the ability to gauge the effectiveness of risk mitigation techniques for current and changing risk factors for each transaction type and level of access.

Although there is no set template for this process, credit unions seeking general information may reference the Small Entity Compliance Guide for the Interagency Guidelines Establishing Information Security Standards (http://www.ffiec.gov/ffiecinfobase/resources/info_sec/2006/ots-ceo-ltr-231.pdf)

Risk Assessment—Continued

and the FFIEC IT Examination Handbook, Information Security Booklet (http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/e_banking.pdf).

Since many credit unions outsource their electronic banking applications, you may be curious whether your provider can complete this assessment. The answer is yes, provided your credit union understands it is ultimately responsible for managing risk and should perform appropriate due diligence as required when selecting a service provider. You may accept the risk assessment performed by your provider after management has ensured the assessment is accurate and the solutions are sufficient to mitigate the risks to your members.

Authentication

The FFIEC has determined that single-factor authentication is inadequate for high risk transactions involving member information or movement of funds to other parties and/or accounts. Therefore, if your electronic banking applications "permit the movement of funds to other parties and/or the access to customer information…it is 'high risk', necessitating stronger authentication or additional controls", according to the FFIEC.

The following techniques may be used to enhance your authentication standards:

- Shared Secrets – Such as customer selected images
- Smart Cards / Tokens
- Biometrics – Fingerprint Scanners
- Internet Protocol Address (IPA) verification
- Mutual Authentication – Member identity and credit union website is authenticated

Other techniques are listed in the guidance referenced above. Credit unions should implement an adequate authentication process prior to year end 2006.

Monitoring

A sound authentication system includes audit features that can assist in the detection of fraud, money laundering, compromised passwords, or other unauthorized activities. Although all credit unions should already have transaction monitoring procedures in place to comply with current Bank Secrecy Act regulations, credit unions will need to enhance their procedures to specifically address:

- Identifying unauthorized transactions
- Detecting intrusions
- Reconstructing events
- Promoting employee & user accountability
- Identifying suspicious patterns

If these services are outsourced to a third party, management must ensure proper logging and monitoring procedures are in place and that suspicious or unauthorized activates are relayed to management in a timely manner.

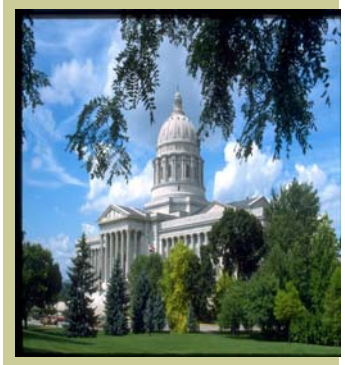
Information and Technology Update

Recent advances in technology are forcing many credit unions, large and small, to provide members with a wider array of services to remain competitive. As a result, credit unions of all sizes have found, in most cases, its much more cost effective to rely on external service providers for these enhanced technology-related services, such as websites & online banking.

As the Division continues to perform random Information Systems and Technology exams, a recurring concern is becoming apparent: Lack of Third Party Due Diligence. It appears that since these functions are performed by organizations outside the financial institution, risk associated with outsourcing arrangements may either be realized in a different manner or may not be recognized at all, than if these functions were performed in-house. Outsourced relationships should be subject to the same policies that would be expected if the credit union were conducting the activities in-house. Therefore, it is managements' responsibility to develop procedures to monitor and mitigate risks associated with outsourced relationships, such as loss of funds, loss of competitive advantage, damaged reputation, improper disclosure of information, and regulatory action. The following should be included within your third-party due diligence program:

- Implement policies / procedures when entering into a third-party agreement, including:
  - Obtaining legal counsel to review the contract,
  - Verifying financial stability,
  - Considering risks of third party subcontracting or using multiple service providers
  - Requiring references from other institutions regarding a particular provider's reputation.
- Establish a risk management program / process, to identify ongoing risk with each third party. Credit Unions are encouraged to periodically rank service providers according to risk to determine who requires closer monitoring.
- Obtain annual financials from service providers to determine financial strength
- Evaluate the adequacy of a provider's internal security controls. Generally, this would include obtaining Type II SAS70 reports. If SAS70 reports are not available, the credit union should either obtain reasonable assurance of the provider's internal controls, or reevaluate the relationship.
- Ensure all third party service providers practice adequate business continuity planning. The credit union should understand all relevant service provider business continuity requirements, incorporate those requirements within its own business continuity plan, and ensure the service provider tests its plan annually.

Relationships with third-party service providers, in many cases, can be very beneficial to the membership, however not subjecting these relationships to the same policies and procedures for in-house services can open your credit union up to unnecessary risk. If you would like more information, you may either reference NCUA guidance, such as Letter No: 01-CU-20, or call our office.



DEPARTMENT OF INSURANCE, FINANCIAL INSTITUTIONS AND PROFESSIONAL REGISTRATION

301 West High Street
Suite 720-A
P.O. Box 1607
Jefferson City, MO 65102

Phone: 573-751-3419
Fax: 573-751-6834
E-mail: cu@cu.mo.gov

Www..cu.mo.gov